UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/981,760	10/19/2001	Toshihiko Ninomiya	500.40788X00	6674

20457 7590 03/25/2005

ANTONELLI, TERRY, STOUT & KRAUS, LLP
1300 NORTH SEVENTEENTH STREET
SUITE 1800
ARLINGTON, VA 22209-3873

EXAMINER	
HO, THOMAS M	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 03/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/981,760	NINOMIYA ET AL.	
	Examiner	Art Unit	
	Thomas M Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *19 October 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 2.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-12 are pending.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 4- 6, 11, 12 are rejected under 35 U.S.C. 112 2nd paragraph as being indefinite.

Applicant has recited "public key and a secret key of a public key cryptosystem". If applicant intends to call a "secret key" a "private key", the Examiner should note that this interpretation is different from the established definition in the art. (Column 4, lines 15-32) of Saito, US patent 6,002,772 clarifies the differences between the two systems. A secret key system is a system in which a single key is used for both encryption and decryption. A public key crypto system employs one key for use in encryption and another key for use in decryption. The secret key and public key are two different systems, and public key cryptosystems do not have secret keys.

However labeling a "secret key" a "private key" is so common of a mistake (analogous to misnterpreting "fortuitous" as "fortunate") that Examiner finds the interpretation of "secret key" as "private key" acceptable because those or ordinary skill in the art would be normally be able to understand what applicant intended in the context of its use.

Nevertheless, the claim is rejected as being indefinite because Examiner is unable to determine whether or not applicant actually intended to call a "secret key" a "private key" or actually mean a secret key.

Claims 6, 11, 12 are rejected for similar reasons.

Claim 5 is rejected as being dependent upon claim 4.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-2 are rejected under 35 U.S.C. 102(b) as being anticipated by Saito, US patent 6,002,772.

In reference to claim 1:

Saito discloses a cryptographic key management method comprising steps of:

- Generating and storing a management cryptographic key, where the management cryptographic key is the public key. (Column 6, lines 60-67)

- Generating a transaction cryptographic key with the management cryptographic key, where the transaction cryptographic key is the private key, Ks1. (Column 6, lines 60-67)
- Encrypting the transaction cryptographic key with the management cryptographic key, where public key is used to encrypt the private key, KS1. (Column 6, lines 60-67)
- Storing the encrypted transaction cryptographic key in a key management server, where the key management center stores the encrypted cryptographic keys. (Column 6, lines 60-67)

In reference to claim 2:

Saito (Column 6, lines 60-67) discloses a cryptographic key management method according to claim 1, wherein if a plurality of transaction cryptographic keys are generated, each of the transaction cryptographic keys is encrypted with the management cryptographic key, where the plurality of cryptographic keys is KS1 and KS2, and both are encrypted with the public key.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 3, 7-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Saito.

In reference to claim 3:

Saito discloses a cryptographic key management method according to claim 1, further comprising steps of:

- Acquiring the encrypted transaction cryptographic key from the key management server, where the encrypted key KS1 is acquired from the key management center and sent to the client. (Column 7, lines 1-4)
- Acquiring the transaction cryptographic key. (Column 7, lines 5-10)

Saito fails to explicitly disclose:

Decrypting the encrypted transaction cryptographic key with the management cryptographic key.

- Saito however does disclose decrypting the encrypted transaction cryptographic key with the user private key, the counterpart to the management key. (Column 7, lines 5-10)

The Examiner takes official notice that secret key cryptography as an alternative to public key cryptography was well known at the time of invention. Secret key cryptography involves encrypting and decrypting with a single key, while public key cryptography involves encrypting with public key and decrypting with a private key (although this may be reversed for certain scenarios like digital signatures) Saito discloses secret key cryptography in the background of the invention, (Column 4, lines 15-25)

It would have been obvious to one of ordinary skill in the art at the time of invention to use secret key cryptography and both encrypt and decrypt the transaction key in order to simplify the encryption/decryption process with using only a single key.

Claim 7 is rejected for the same reasons as claim 3.

Claim 8 is rejected for the same reasons as claim 2.

In reference to claim 9:

Saito fails to discloses a network system according to claim 7, wherein:

- Said client sends to a valid term of the encrypted transaction cryptographic key together with the encrypted transaction cryptographic key to the key server;
- Said key server notifies an expiration of the valid term of the transaction cryptographic key.

The Examiner takes official notice that establishing a valid term for keys and expiration of these terms was well known in the art at the time of invention. Keys expire over time and need to be updated. US patent 5261002, Perlman (Column 4, lines 5-18) for example discloses a start time and when the certificate containing a public key is to be considered invalid.

It would have been obvious to one of ordinary skill in the art at the time of invention to set a valid term on the encrypted transaction cryptographic key and have the server notify an

expiration of the valid term, to provide greater security and prevent a key from being compromised by updating and changing it from time to time.

In reference to claim 10:

Saito fails to discloses a network system according to claim 7, wherein:

- Said client sends the maximum number of use time of the transaction cryptographic key together with the encrypted transaction cryptographic key to said key server;
- Said key server counts the number of acquisition requests for the encrypted transaction cryptographic key and notifies uses over the maximum number to said client.

The Examiner take official notice that placing a counter for the usage of a cryptographic key was well known at the time of invention. US patent 4866707 (Column 7, lines 24-30) discloses an example of this. The purpose of having a key counter is so that there is a maximum number of times a key may be used. This is also common in content distribution systems where a client may purchase a "pay per view" for particular content descrambling.

It would have been obvious to one of ordinary skill in the art for the client to include a max use time along with the key, and have the server count the number of uses and notify the client in order to allow a means to limit a clients usage for content, thereby allowing a client to only "rent" the use of key which may be cheaper.

Conclusion

7. The following art not relied upon is made of record:

- US patent 5745572 discloses a cryptographic key management method.
- US patent 6577734 discloses a data encryption key management system.
- US patent 6072876 discloses a method of depositing a key in a separate server.

8. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (571)272-3838.

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist	Telephone: 571-272-2100	Fax: 703-872-9306
Customer Service Representative	Telephone: 571-272-2100	Fax: 703-872-9306

TMH

March 19th, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100